Yee & Associates, P.C.

13760 Noel Road
Suite 900
Dallas, Texas 75240

Main No. (972) 367-2001
Facsimile (972) 367-2008

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Thomas M. Ho** **Group Art Unit 2134**	Facsimile No.: **703/872-9306**
From: Michele Morrow Legal Assistant to Gerald H. Glanzman	No. of Pages Including Cover Sheet: **25**
Message: Enclosed herewith: • Transmittal Document; and • Appeal Brief.	
Re: Application No. **09/620,350** Attorney Docket No: **AUS990912US1**	
Date: Tuesday, October 19, 2004	
Please contact us at (972) 367-2001 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-367-2008.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Reid**

Serial No.: **09/620,350**

Filed: **July 20, 2000**

For: **System, Apparatus and Method for Updating Security Configurations of a Plurality of Servers from a Centralized Directory Server**

§
§
§
§
§
§
§
§
§

Group Art Unit: **2134**

Examiner: **Ho, Thomas M.**

Attorney Docket No.: **AUS990912US1**

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on October 19, 2004.

By: Michele Morrow
Michele Morrow

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37).

A fee of $340.00 is required for filing an Appellant's Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,

Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 367-2001
ATTORNEY FOR APPLICANT

RECEIVED
CENTRAL FAX CENTER

OCT 19 2004

Docket No. AUS990912US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Reid**	§	
	§	Group Art Unit: **2134**
Serial No. **09/620,350**	§	
	§	Examiner: **Ho, Thomas M.**
Filed: **July 20, 2000**	§	
	§	
For: **System, Apparatus and Method for Updating Security Configurations of a Plurality of Servers from a Centralized Directory Server**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (703) 872-9306 on October 19, 2004.

By: Michele Morrow
Michele Morrow

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on August 20, 2004.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-40

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: NONE
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-40
4. Claims allowed: NONE
5. Claims rejected: 1-40

C. CLAIMS ON APPEAL

The claims on appeal are: 1-40

STATUS OF AMENDMENTS

An Amendment after Final Rejection was not filed. Therefore, claims 1-40 on appeal herein areas amended in the Response to Office Action filed February 26, 2004.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The subject matter of claim 1 is directed to a method of updating security configurations of a plurality of servers from a centralized server. A system in which the invention may be implemented is illustrated in **Figure** 1 and is described beginning on page 6, line 5 and extending to page 10, line 4. The method is illustrated in **Figure 4** and is described beginning on page 13, line 29 and extending to page 14, line 23. According to the invention, when the security configuration of a plurality of servers **120, 130, 140** is to be updated with changed security information, security information is first changed in a centralized server **150** (see page 14, lines 6-9, Step **410** in **Figure 4**). In response to receiving an update command (see page 14, lines 9-13, Step **420** in **Figure 4**), the changed security information is downloaded to the plurality of servers **120, 130, 140** in order to update the security configuration of each of the plurality of servers **120, 130, 140** (see page 14, lines 14-22, Step **430** in **Figure 4**). The present invention permits the security configuration of a plurality of servers to be changed from a centralized database in a relatively automated fashion, and makes it unnecessary to separately change the security configuration of each of the plurality of servers.

B. CLAIM 12 – INDEPENDENT

The subject matter of claim 12 is directed to a security configuration update server for updating security configurations of a plurality of servers. The security configuration update server is illustrated in detail in **Figure 2** and described beginning on page 10, line 5 and extending to page 11, line 16. Security configuration update server **150** includes controller **210**, network interface **220** coupled to controller **210**, and storage device **230** coupled to controller **210**. In response to receiving an update command, controller **210** downloads security information stored in storage device **230** to the plurality of servers **120, 130, 140** illustrated in **Figure 1** via network interface **220** in order to update the security configuration of each of the plurality of servers **120, 130, 140.**

C. CLAIM 23 – INDEPENDENT

The subject matter of claim 25 is directed to a computer program product in a computer readable medium for updating security configurations of a plurality of servers. The claim is a computer program product counterpart claim to method claim 1.

D. CLAIM 32 – INDEPENDENT

The subject matter of claim 32 is directed to a method for updating the security configuration of a plurality of servers **120, 130, 140**. The method is illustrated in **Figure 4** and described beginning on page 13, line 29 and extending to page 14, line 23. Changes to access information are collected to form modified access information (Step **410** in **Figure 4**). In response to a policy, the modified access information is transferred to the plurality of servers **120, 130, 140** (Step **430** in **Figure 4**) and used to update the security configuration of the plurality of servers. The manner in which the plurality of servers update their security configuration is illustrated in **Figure 5** and described beginning on page 14, line 24 and extending to page 25, line 6.

E. CLAIM 37 – INDEPENDENT

The subject matter of claim 37 is directed to a data processing system, and is, substantially, a system claim counterpart to method claim 1.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION 1 (Claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35, 37-40)

Claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35 and 37-40 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,956,715 (Glasser et al.).

B. GROUND OF REJECTION 2 (Claims 7, 9, 18, 20, 28, 30, 34, 36)

Claims 7, 9, 18, 20, 28, 30, 34 and 36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,956,715 (Glasser et al.).

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35, 37-40)

Glasser et al. (hereinafter Glasser) discloses a technique for managing file and other resource security in a networked computing environment. The network includes server computers, each of which controls a particular resource that is shareable among users of the network. A resource may be organized as a hierarchy of elements, and a procedure is described for changing security protection; e.g., access authorization, to an element in the hierarchy.

In rejecting the claims as being anticipated by Glasser, the Examiner states the following:

> Glasser et al. discloses a method of updating security configurations of a plurality of servers, comprising:
>
> · Changing security information in a centralized server, where the security information is the commands for manipulating resource access permissions (Column 7, lines 45-48)
>
> · Receiving an update command (Column 7, lines 46-48)
>
> · Downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers, where the downloaded information occurs when the security information is propagated down the network (Column 7, lines 60-65)

Final Office Action dated May 24, 2004, pages 6 and 7.

Claim 1 of the present application reads as follows:

> 1. A method of updating security configurations of a plurality of servers, comprising:
> changing security information in a centralized server;
> receiving an update command; and
> downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers.

Glasser does not disclose "changing security information in a centralized server". Instead, Glasser generally discloses changing security information for a particular server at the server. For example, in Col. 7, lines 46-48, Glasser states that when changing access permission to a

resource controlled by peer server **120**, "[c]ommands for manipulating resource access permissions are assumed to be received from user interface **125** of peer server **120**". Thus, security information is not changed in a centralized server but is changed at server **120** itself via GUI **125** associated with the server.

Although, as pointed out by the Examiner, the commands can also come from a remote source or from another node of the network (col. 7, lines 48-54 of Glasser), the change in access information for the resource stored on hard disk **121** is still being made in peer server **120** and not from a centralized server.

Glasser also does not disclose "downloading the changed security information to the plurality of servers in response to receiving the update command". Again, in Glasser, security information appears to be downloaded to a resource associated with a particular server from that particular server, not to a plurality of servers in response to an update command.

Accordingly, in Glasser, there is no centralized server in which security information is changed, and no downloading of changed security information from a centralized server to a plurality of servers (such as, for example, peer servers **120** and **140** in Glasser). In Glasser, security information is changed at each server.

In rejecting the claims, the Examiner appears to contend that files stored on hard disk **121** associated with peer server **120** are arranged in a hierarchical manner, and that the files themselves can be construed as "servers". The Examiner then contends that Glasser can be construed as reading on claim 1 by virtue of changed security information being downloaded from one file to another through the hierarchy. In particular, the Examiner states:

> Thus, the aspect of the server computer that makes it a "server" lies within the ability to provide a resource or resources to clients. The Examiner maintains then that the file and folder system as disclosed by Glasser (Figure 9), can indeed be construed as servers since it is from the folders from which a client may access a particular resource such as files. Additionally, the folders themselves are even disclosed to contain individual access control lists. Thus each folder is also individual point of authentication and authorization, further implying each folder as a separate conceptual entity

Final Office Action dated May 24, 2004, page 5.

Appellant respectfully disagrees with the Examiner's interpretation of Glasser. Figure 4 of Glasser is as follows:

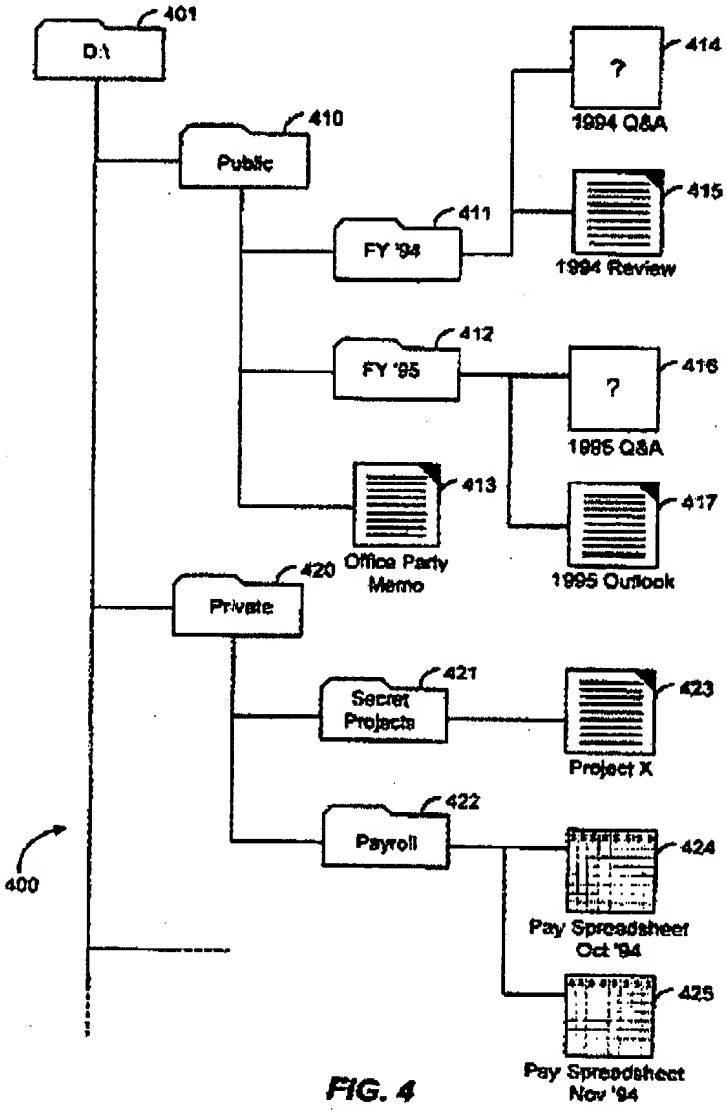

FIG. 4

As shown in Figure 4 of Glasser, hierarchy **400** comprises a plurality of files and folders **401**, **410**, **411**, etc., stored on hard disk **121** associated with peer server **120**. Some of the files and folders have an access control list (ACL), while other folders and files inherit an ACL from

the nearest ancestor folder or file having an ACL.

In Column 7, lines 55-58, Glasser reads:

> "Initially, the resource for which permissions are to be established or modified is selected (step A). Peer server **120** receives a command to change the permissions for the selected resource (step B)."

In Glasser, peer server **120** receives a command to change the permissions for a selected resource. Peer server **120** then determines if the resource, e.g., a particular folder, has its own ACL. If so, the folder's own ACL is updated. If not, the nearest ancestor having an ACL is determined, and that ACL is updated.

The individual files and folders **401**, **410**, **411**, etc., are not servers even though they may be arranged in a hierarchical manner. Files and folders **401**, **410**, **411**, etc., in Glasser are simply resources stored on hard disk **121**, and cannot reasonably be construed as servers. Furthermore, even if the files and folders stored on hard disk **121** could be considered as being "servers", and Appellant disagrees that this is a reasonable interpretation of a "server" as that term is used in the data processing field, security information is still being changed only in an ACL for a particular folder or file. Changed security information is not being downloaded from a centralized server to a plurality of servers in response to receiving an update command as recited in claim 1.

For at least all the above reasons, Glasser does not anticipate claim 1, and claim 1 should be allowable over Glasser in its present form.

Claims 2-6, 8, 10 and 11 depend from and further restrict claim 1 and are also not anticipated by Glasser, at least by virtue of their dependency.

Independent claim 12 recites a controller and a storage device coupled to the controller. In addition, claim 12 recites that the controller, in response to receiving an update command, downloads security information stored in the storage device to a plurality of servers via a network interface. Claim 12 is not anticipated by Glasser for reasons similar to those discussed above with respect to claim 1, and claim 12, together with claims 13-17, 19, 21 and 22 dependent thereon, are also believed to be allowable over Glasser in their present form.

Independent claims 23, 32 and 37 contain limitations similar to those discussed above with respect to claims 1 and 12, and are also not anticipated by Glasser for substantially the same reasons as discussed above with respect to claims 1 and 12.

Claims 24-27, 29, 31, 33, 35 and 38-40 depend from and further restrict one of independent claims 23, 32 and 37, and are also not anticipated by Glasser, at least by virtue of their dependency.

Therefore, claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35, 37-40 are believed to patentably distinguish over Glasser, and it is respectfully requested that the Board reverse the Examiner's final rejection of those claims.

B. GROUND OF REJECTION 2 (Claims 7, 9, 18, 20, 28, 30, 34, 36)

The Examiner has rejected claims 7, 9, 18, 20, 28, 30, 34 and 36 under 35 U.S.C. § 103(a) as being unpatentable over Glasser. In rejecting these claims, the Examiner takes official notice that receiving update commands at scheduled periodic times is well-known to those of ordinary skill in the art; and, further, that lightweight directory access protocol (LDAP) is well known to those of ordinary skill in the art.

These claims all depend from and further restrict independent claims. The matters of which the Examiner takes official notice do not supply the deficiencies in Glasser with respect to the independent claims, as discussed in detail above; and for at least the reasons discussed above, claims 7, 9, 18, 20 28, 30, 34 and 36 are not obvious in view of Glasser, and should be allowable in their present form.

Therefore, claims 7, 9, 18, 20, 28, 30, 34, 36 are believed to patentably distinguish over Glasser, and it is respectfully requested that the Board reverse the Examiner's final rejection of those claims.

Gerald H. Glanzman
Reg. No. 25,035
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 367-2001

APPENDIX OF CLAIMS

The text of the claims involved in the appeal are:

1. A method of updating security configurations of a plurality of servers, comprising:

changing security information in a centralized server;

receiving an update command; and

downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers.

2. The method of claim 1, wherein the plurality of servers are Windows NT servers and the centralized server is a directory server.

3. The method of claim 1, wherein the centralized server is a directory server and wherein changing the security information includes using an editor to change a directory listing in the centralized server.

4. The method of claim 1, wherein the security configurations of the plurality of servers are updated by updating security parameter lists associated with at least one of files and resources associated with each of the plurality of servers.

5. The method of claim 4, wherein the security parameter lists identify authorized users or authorized groups of users of the at least one of files and resources associated with the security parameter lists.

6. The method of claim 1, wherein the update command is received from a network administrator.

7. The method of claim 1, wherein the update command is received at scheduled periodic times.

8. The method of claim 1, wherein the update command is received from one or more of the plurality of servers.

9. The method of claim 1, wherein the centralized server is a light weight directory access protocol server.

10. The method of claim 1, wherein downloading the changed security information includes filtering a directory listing stored on the centralized server to extract the changed security information.

11. The method of claim 1, wherein the security configurations are updated by filtering the downloaded changed security information to extract only necessary update information for updating the security configurations and then updating the security configurations based on the extracted necessary update information.

12. A security configuration update server for updating security configurations of a plurality of servers, comprising:

a controller;

a network interface coupled to the controller; and

a storage device coupled to the controller, wherein the controller, in response to receiving an update command, downloads security information stored in the storage device to the plurality of servers via the network interface, wherein the downloaded security information is used to update the security configurations of the plurality of servers.

13. The security configuration update server of claim 12, wherein the plurality of servers are Windows NT servers and the security configuration update server is a directory server.

14. The security configuration update server of claim 12, wherein the update command includes changes to the security information.

15. The security configuration update server of claim 12, wherein the security configuration of the plurality of servers are updated by updating security parameter lists associated with at least one of files and resources associated with each of the plurality of servers.

16. The security configuration update server of claim 15, wherein the security parameter lists identify authorized users or authorized groups of users of the at least one of files and resources associated with the security parameter lists.

17. The security configuration update server of claim 12, wherein the update command is received from a network administrator.

18. The security configuration update server of claim 12, wherein the update command is received at scheduled periodic times.

19. The security configuration update server of claim 12, wherein the update command is received from one or more of the plurality of servers.

20. The security configuration update server of claim 12, wherein the security configuration update server is a light weight directory access protocol server.

21. The security configuration update server of claim 12, wherein downloading the changed security information includes filtering a directory listing stored in the storage device to extract the changed security information.

22. The security configuration update server of claim 12, wherein the security configurations are updated by filtering the downloaded security information to extract only necessary update

information for updating the security configurations and then updating the security configurations based on the extracted necessary update information.

23. A computer program product in a computer readable medium for updating security configurations of a plurality of servers, comprising:

first instructions for changing security information in a centralized server;

second instructions for receiving an update command; and

third instructions for downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers.

24. The computer program product of claim 23, wherein the centralized server is a directory server and wherein the first instructions include instructions for using an editor to change a directory listing in the centralized server.

25. The computer program product of claim 23, wherein the third instructions include instructions for updating security parameter lists associated with at least one of files and resources associated with each of the plurality of servers.

26. The computer program product of claim 25, wherein the security parameter lists identify authorized users or authorized groups of users of the at least one of files and resources associated with the security parameter lists.

27. The computer program product of claim 23, wherein the update command is received from a network administrator.

28. The computer program product of claim 23, wherein the update command is received at scheduled periodic times.

29. The computer program product of claim 23, wherein the update command is received from one or more of the plurality of servers.

30. The computer program product of claim 23, wherein the centralized server is a light weight directory access protocol server.

31. The computer program product of claim 23, wherein the third instructions include instructions for filtering a directory listing stored on the centralized server to extract the changed security information.

32. A method in a data processing system for updating access information for a plurality of servers, the method comprising:

collecting changes to access information at the data processing system to form modified access information; and

responsive to a policy, transferring the modified access information to the plurality of servers, wherein the modified access information is used to update the security configurations of the plurality of servers.

33. The method of claim 32, wherein the policy comprises receiving a request to update the security configurations for the plurality of servers.

34. The method of claim 32, wherein the policy comprises periodically initiating transfer of modified access information to the plurality of servers.

35. The method of claim 32, wherein the policy comprises initiating the transfer of the modified access information to the plurality of servers in response to a selected event.

36. The method of claim 35, wherein the selected event is a periodic event.

37. A data processing system, comprising:

a centralized server; and

a plurality of servers coupled to the centralized server by at least one network, wherein the centralized server stores security information, and wherein when the centralized server receives an update command, the security information stored in the centralized server is downloaded to at least one of the plurality of servers, the downloaded security information being used by the at least one of the plurality of servers to update the security configurations of the at least one of the plurality of servers.

38. The system of claim 37, wherein the plurality of servers are Windows NT servers and the centralized server is a directory server.

39. The system of claim 37, wherein the security configuration of the at least one of the plurality of servers is updated by updating a security parameter list associated with at least one of files and resources associated with the at least one of the plurality of servers.

40. The system of claim 37, wherein the security information is filtered by the centralized server, prior to downloading the security information, to extract only security information that has been changed.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.